	<b>Kryptographie</b>	it.schule stuttgart Breitwiesenstrasse 20-22 70565 Stuttgart
	Übung – Symmetrische Kryptographie	

Im vergangenen Jahr war viel über die Aktivitäten verschiedener Geheimdienste und deren Bestreben zu lesen, nahezu die gesamte Kommunikation über das Internet zu überwachen. Unter einem diffusen Gefühl des Unbehagens leidend, beschließen Sie, sich mit den Grundlagen der Kryptographie vertraut zu machen.

Ihr erstes Ziel besteht darin, bei Bedarf sicher verschlüsselte Nachrichten mit einem Gegenüber austauschen zu können.

Ursprünglich bezeichnete Kryptographie die Wissenschaft der Verschlüsselung von Informationen. Klassisch kann man die Kryptographie in zwei Bereiche untergliedern. Die symmetrische und die asymmetrische Kryptographie.

## Symmetrische Kryptographie

Symmetrische Verfahren der Kryptographie sind bereits seit dem Altertum bekannt und entsprechen vermutlich den intuitiven Vorstellungen der meisten Menschen darüber, wie der Austausch geheimer Nachrichten erfolgen kann. Stark vereinfacht ausgedrückt werden dabei die folgenden Schritte durchlaufen:

1. Eine Klartext-Nachricht wird mittels eines geheimen Schlüssels und eines Verschlüsselungsalgorithmus zunächst in eine Chiffretext-Nachricht (verschlüsselte Nachricht) verwandelt.
2. Anschließend wird die Chiffretext-Nachricht über einen unsicheren Kanal oder ein unsicheres Medium (z.B. das Internet) verschickt.
3. Schließlich wird die Chiffretext-Nachricht vom Empfänger (der sowohl den geheimen Schlüssel, als auch den passenden Entschlüsselungsalgorithmus kennen muss) wieder in die ursprüngliche Klartext-Nachricht zurückverwandelt.

### **Aufgabe 1: Senden Sie eine (stark) verschlüsselte Nachricht an eine befreundete Gruppe**

Gehen Sie paarweise zusammen und bilden Sie 2er-Gruppen. Ihre Aufgabe besteht nun darin, sich eine weitere Gruppe als Adressat für Ihre verschlüsselte Nachricht auszusuchen und dieser dann eine (beliebige) verschlüsselte Nachricht zu senden.

Diese Aufgabe gilt als gelöst, sobald es Ihrer Adressaten-Gruppe gelungen ist Ihre Nachricht erfolgreich zu dechiffrieren.

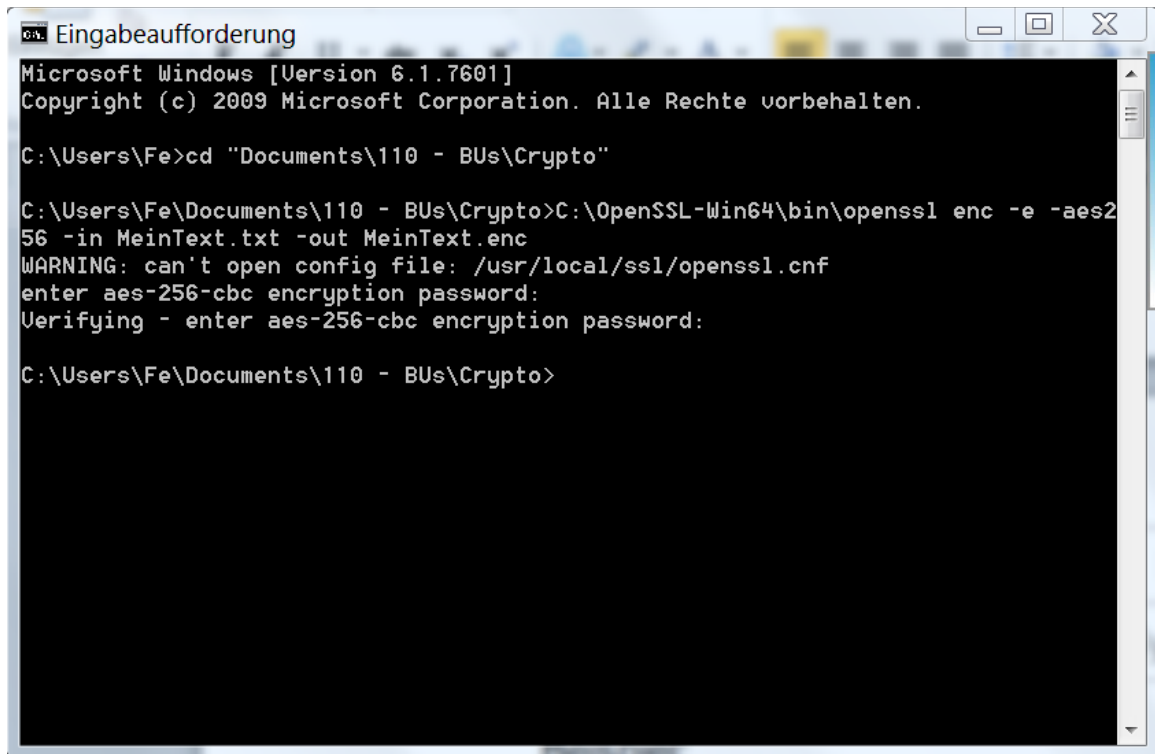
Zur Verschlüsselung Ihrer Nachricht gehen Sie wie folgt vor:

1. Laden Sie das Programmpaket OpenSSL (Win64 OpenSSL v1.0.2e) für Windows von der Seite <https://slproweb.com/products/Win32OpenSSL.html> herunter und installieren Sie das Paket auf ihrem lokalen Rechner.
2. Erstellen Sie in Ihrem persönlichen Verzeichnis den Ordner Crypto
3. Legen Sie in diesem Ordner eine Datei mit dem Namen MeinText.txt mit einem Texteditor an. Erstellen Sie in dieser Datei eine „geheime Nachricht“.
4. Verschlüsseln Sie die Datei indem Sie die Eingabeaufforderung öffnen, in Ihren Crypto-Ordner wechseln und folgenden Befehl eingeben:

```
openssl enc -e -aes256 -in MeinText.txt -out MeinText.enc
```

Achten Sie dabei darauf, dass der Befehl openssl möglicherweise nicht genügt, sondern Sie ggf. den kompletten Pfad zum Programm angeben müssen und Sie außerdem zuvor in Ihren „Crypto“-Ordner wechseln sollten, der Ihre Datei MeinText.txt enthält.

Beispiel:



```

Eingabeaufforderung
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Users\Fe>cd "Documents\110 - BUs\Crypto"

C:\Users\Fe\Documents\110 - BUs\Crypto>C:\OpenSSL-Win64\bin\openssl enc -e -aes2
56 -in MeinText.txt -out MeinText.enc
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
enter aes-256-cbc encryption password:
Verifying - enter aes-256-cbc encryption password:

C:\Users\Fe\Documents\110 - BUs\Crypto>

```

5. Öffnen Sie die Datei MeinText.enc und prüfen Sie, ob die Inhalte erfolgreich verschlüsselt wurden.
6. Senden Sie die Datei an die Gruppe, die Ihre Nachricht entschlüsseln soll. Nutzen Sie dazu entweder Ihren E-Mail-Account oder das Tauschlaufwerk.
7. Leiten Sie in geeigneter Weise die notwendigen Informationen an die Empfängergruppe weiter, die diese benötigt um Ihre Nachricht zu entschlüsseln.

Zum Dechiffrieren der Nachricht gehen Sie wie folgt vor:

1. Nutzen Sie den Befehl:


```
openssl enc -d -aes256 -in MeinText.enc -out MeinText.txt
```

Achten Sie dabei auf vollständige Pfadangaben bzw. das richtige Arbeitsverzeichnis.

## **Aufgabe 2:**

Beantworten Sie folgende Fragen (recherchieren Sie dazu ggf. im Internet):

1. Welches ist der vermutlich bekannteste im Altertum benutzte symmetrische Verschlüsselungsalgorithmus? Wie schätzen Sie die Sicherheit dieses Algorithmus heutzutage ein?
2. Welchen Verschlüsselungsalgorithmus haben Sie in Aufgabe 1 genutzt?
3. Wie schätzen Sie die Sicherheit des Verschlüsselungsalgorithmus aus Aufgabe 1 ein?

	<b>Kryptographie</b>	it.schule stuttgart Breitwiesenstrasse 20-22 70565 Stuttgart
	Übung – Symmetrische Kryptographie	

4. Stellen Sie sich vor, Ihre Adressatengruppe hätte sich nicht im selben Raum befunden - vor welcher Herausforderung stünden Sie?
5. Stellen Sie sich weiter vor, Sie arbeiteten im „Geheimdienst ihrer Majestät“ und Sie müssten sicherstellen, dass mehrere tausend Agenten wechselseitig sicher miteinander kommunizieren können. Wie entwickelt sich die Herausforderung aus Aufgabe 4 unter diesen Umständen?
6. Angenommen Sie benutzen einen sehr sicheren Verschlüsselungsalgorithmus, welcher Versuchung könnten Sie erliegen, die es Angreifern ermöglicht Ihre Nachricht dennoch in relativ kurzer Zeit zu dechiffrieren? Wie nennt man solche Angriffe?
7. Einige weit verbreitete Anwendungs-Programme verfügen über „eingebaute“ symmetrische Kryptographie – können Sie einige Beispiele nennen und haben Sie derartige Funktionen evtl. bereits selbst genutzt?
8. Bei welcher Gruppe derartiger Programme ist diese Funktion („eingebaute symmetrische Kryptographie“) besonders sinnvoll? Nennen Sie Gründe die dennoch dafür sprechen stattdessen OpenSSL zu verwenden.